Authenticated Key Agreement Based on NFC for Mobile Payment

Bomi Seo[1], Sung Woon Lee[2]*, Hyunsung Kim[1]

[1] The Department of Cyber Security, Kyungil University, Korea.
[2] The Department of Information Security, Tongmyoung University, Korea.

* Corresponding author. Tel.: +82 10-6340-0587; email: staroun@tu.ac.kr
Manuscript submitted October 2, 2014; accepted May 25, 2015.
doi: 10.17706/ijcce.2016.5.1.71-78

Abstract: Mobile payment is being adopted all over the world in different ways. Along with the increased convenience at the point of sale, mobile payment acceptance can also bring new risks to the security of cardholder data. Authentication is a basic security building block for mobile payment and there are some of research results, which were proven to be weak against attacks. This paper proposes a new authenticated key agreement based on NFC for mobile payment to solve the problems in the previous researches. The proposed scheme is secure against various attacks and could provide privacy to the participants.

Key words: Security, mobile payment, authenticated key agreement, near field communication.

1. Introduction

Mobile payment is being adopted all over the world in different ways, which generally refer to payment services operated under financial regulation and performed from or via a mobile device [1]-[3]. In 2008, the combined market for all types of mobile payments was projected to reach more than $600B globally by 2013, which would be double the figure as of February, 2011. The mobile payment market for goods and services, excluding contactless near field communication (NFC) or NFC transactions and money transfers, is expected to grow exponentially through 2015. Along with the increased convenience at the Point of Sale, mobile payment acceptance can also bring new risks to the security of cardholder data. Securing account data at the point of capture is one way that you can actively help in controlling these risks [4]-[6]. There are new security risks introduced with mobile banking and payments that must be identified and mitigated. There are risks that have both an existing mitigation method as well as those that do not have a clear risk mitigation solution [5].

NFC is not accepted by the current market. NFC requires hardware infrastructure support from handset companies and only a small fraction of existing mobile phones have been enabled with this technology. NFC approach is only convenient to on-site payment, therefore, not a convenient and ubiquitous foundation for remote payment. Its security based on locality is questionable since malicious parties can sometimes get close to honest devices/parties. NFC, by its very nature, cannot be used at a distance as in on-line payment. If the NFC hardware infrastructure can be integrated with isolate TransFLash (TF) card, SD card and USB Key, it will be compatible with existing handset [7], [8].

Mobile payment typically consists of providing a credit card number and expiration date at the merchant's website. No additional user authentication is usually required, although sometimes an additional security code printed on the credit card is also requested [9]. A recent offshoot of electronic

commerce, called mobile commerce, has similar needs for secure payment methods. Several user authentication schemes for electronic commerce and mobile commerce are introduced [10]-[13].

This paper proposes a new authenticated key agreement based on NFC (AKA_{NFC}) for mobile payment. We consider a scenario of three parties in the AKA_{NFC}, which are two end users whom share a common authentication server. Two end users could be a buyer or a seller at any period of time, respectively, which does not have any credential in between. Thereby, the authentication server could help them to be authenticated and key establishment between each other. The AKA_{NFC} is secure against various attacks and could provide anonymity and untraceability, which could be used as a security building block for mobile payment.

2. Backgrounds

In this section, we review the network environment of mobile payment, which involves three entities including two users and an authentication center. Also we review some of recent authentication mechanisms to draw research directions of the proposed authentication protocol.

2.1. Mobile Payment Environment

Fig. 1 shows the focusing network configuration of this paper for mobile payment. We consider three entities, two users and an authentication server (*AuC*). It is considered that two end users are registered to a common *AuC*. Two end users could be a buyer or a seller at any period of time, respectively, which does not have any credential in between. Furthermore, we consider that two end users should equipped with NFC module on their hand held device. NFC, as an emerging and promising technology, is an integration of radio frequency identification (RFID) technology with mobile devices. NFC is used mostly in paying for purchases made in physical stores or transportation services. A consumer using a special mobile phone equipped with a smart card waves his (or her) phone near a reader module. Most transactions do not require authentication, but some require authentication using PIN, before transaction is completed. The payment could be deducted from a pre-paid account or charged to a mobile or bank account directly.

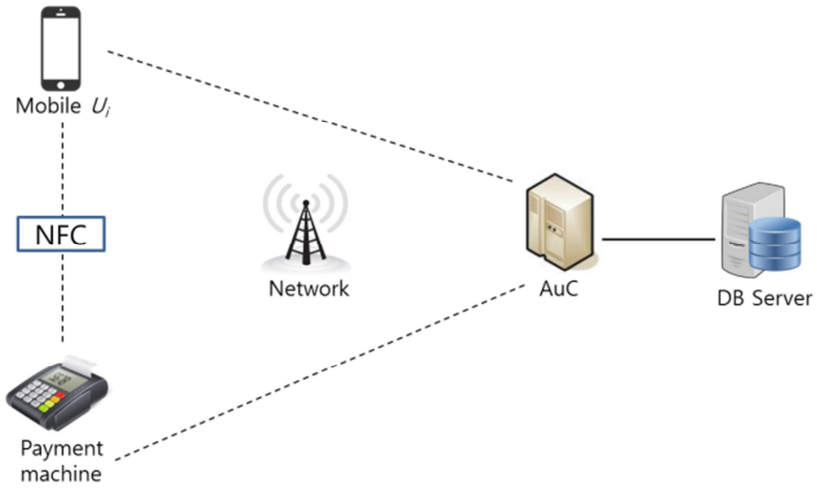

Fig. 1. Focused network environment.

2.2. Related Works

Han *et al*. proposed an electronic payment authentication method using vibration cues, which utilized for design and implementation [10]. They argued that their method enables an efficient, secure mobile payment service by analyzing security issues likely to occur in payments using NFC Smartphone and by

proposing payment protocols with an authentication method using vibration cues to resolve such issues. However Han *et al.*'s method does not consider the privacy issue.

Yadav *et al.* proposed three factors authentication for Android based mobile payment [11]. Yadav *et al.*'s scheme uses what the paying client knows (e.g. secret phrase, password, PIN code), what the paying client has (e.g. token, electronic card, passport), and what the paying client characterizes (e.g. behavioral or biometric feature). They only provide rough steps of the scheme and increase overhead for the authentication to provide high security.

Parte *et al*. proposed multi criterion authentication protocol for mobile payment [12]. However, their authentication is only dependent with the identity and the password, which is a password-based authentication. It does not provide any detailed step for the scheme. Furthermore, it also does not consider the privacy of the participants of the protocol.

Lee *et al*. proposed a NFC based authentication method for defense of the man in the middle attack [13]. Lee *et al.*'s method is based on the public key cryptosystem, which requires the public key infrastructure and does not provide anonymity.

3. Authenticated Key Agreement Based on NFC

This section proposes an authenticated key agreement based on NFC (AKA_{NFC}) for mobile payment. The AKA_{NFC} is divided into two phases, the registration phase and the authenticated key agreement phase. It is considered that the registration is performed at the authentication center for all users with NFC device. Table 1 defines notations used in the AKA_{NFC}.

Table 1. Terminology

Notation	Description
U_i	i number of user devices
ID_i	Identity of an U_i
CID_i	Dynamic identity of an U_i
PW_i	Password of U_i
r_i, a, b, c	Random numbers
PU_{AuC}	Public key of AuC
x	Secret key
g	Group generator over Z_p*
SK	Session key
MAC	Message authentication code
$h()$	Hash function
$\|\|$	Concatenation
$\oplus$	Exclusive or operation

3.1. Registration Phase

When user wants to be registered to the server, he (or she) needs to perform this phase. It is assumed that this phase uses a secure channel between the user, U_i and the authentication server, AuC. The phase as shown in Fig. 2 is performed as follows:

- [RP 1] $U_i \rightarrow AuC$

First of all, U_i inputs his (or her) password PW_i, generates a random number r_i and computes APW_i as in (1). After that, U_i sends $\{ID_i, APW_i\}$ to AuC.

$$APW_i = h(PW_i||r_i) \tag{1}$$

- [RP 2] $AuC \rightarrow U_i$

After receiving the message, *AuC* computes V_i as in (2), where x is the secret key possessed by *AuC*. *AuC* issues a NFC to U_i after it stores $\{V_i, PU_{AuC}\}$ securely in the NFC, where PU_{AuC} in (3) is a public key of *AuC*. U_i stores r_i in the NFC.

$$V_i = h(ID_i||x) \oplus APW_i \tag{2}$$

$$PU_{AuC} = g^x \tag{3}$$

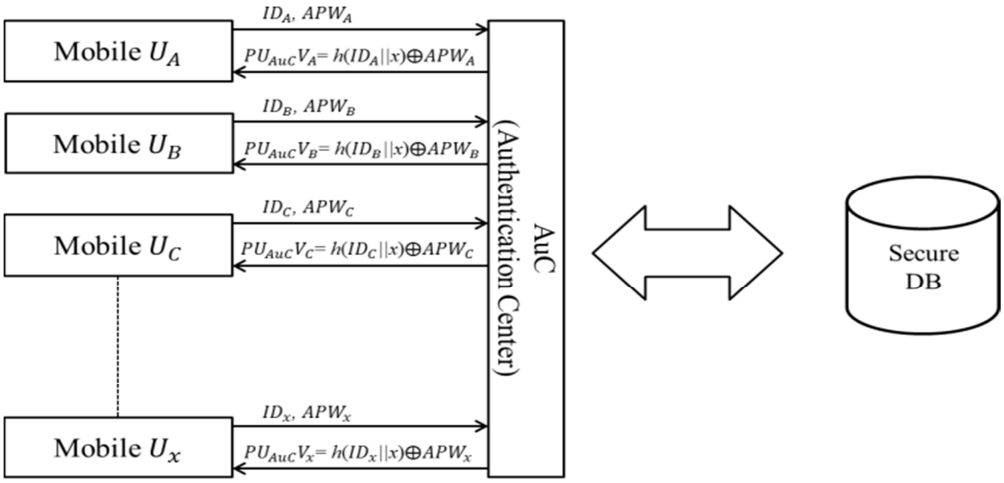

Fig. 2. Registration phase.

3.2. Authenticated Key Agreement Phase

This phase is to establish a secure session key between two mobile devices, U_A and U_B, by helping of *AuC* after the authentication. *AuC* needs to be involved in this phase because U_A and U_B could not believe each other due to no credibility between them. The phase shown in Fig. 3 is performed as follows

- [AP 1] $U_A \rightarrow U_B$

U_A inputs ID_A and PW_A, generates a random number a and computes Y_A as in (4), R_A as in (5), CID_A as in (6) and MAC_A as in (7). After that, U_A sends $\{R_A, CID_A, MAC_A\}$ to U_B.

$$Y_A = V_a \oplus h(PW_A||r_A) \tag{4}$$

$$R_A = g_a \tag{5}$$

$$CID_A = ID_A \oplus (PU_{AuC})^a \tag{6}$$

$$MAC_A = h(Y_A||R_A||ID_A) \tag{7}$$

- [AP 2] $U_B \rightarrow AuC$

U_B inputs ID_B and PW_B, generates a random number b and computes Y_B as in (8), R_B as in (9), CID_B as in (10) and MAC_B as in (11). After that, U_B sends $\{R_B, CID_B, MAC_B, R_A, CID_A, MAC_A\}$ to *AuC*.

$$Y_B = V_B \oplus h(PW_B||r_B) \tag{8}$$

$$R_B = g^b \tag{9}$$

$$CID_B = ID_B \oplus (PU_{AuC})^b \tag{10}$$

$$MAC_B = h(Y_B||R_B||ID_B) \tag{11}$$

- [AP 3] $AuC \rightarrow U_B$

AuC verifies MAC_A and MAC_B. For the verification, it needs to compute ID_A' as in (12), ID_B' as in (13), Y_A' as in (14) and Y_B' as in (15). After that it compares MAC_A and MAC_B with $h(Y_A'||R_A||ID_A')$ and $h(Y_B'||R_B||\mathrm{ID_B}')$. Only if both of the comparisons match, it generates a random number c and computes R_C as in (16), SK_{CA} as in (17), SK_{CB} as in (18), MAC_{CA} as in (19) and MAC_{CB} as in (20). After that, it sends $\{R_C, MAC_{CA}, MAC_{CB}\}$ to U_B.

$$ID_A' = CID_A \oplus {R_A}^x \tag{12}$$

$$ID_B' = CID_B \oplus {R_B}^x \tag{13}$$

$$Y_A' = h(ID_A'||x) \tag{14}$$

$$Y_B' = h(ID_B'||x) \tag{15}$$

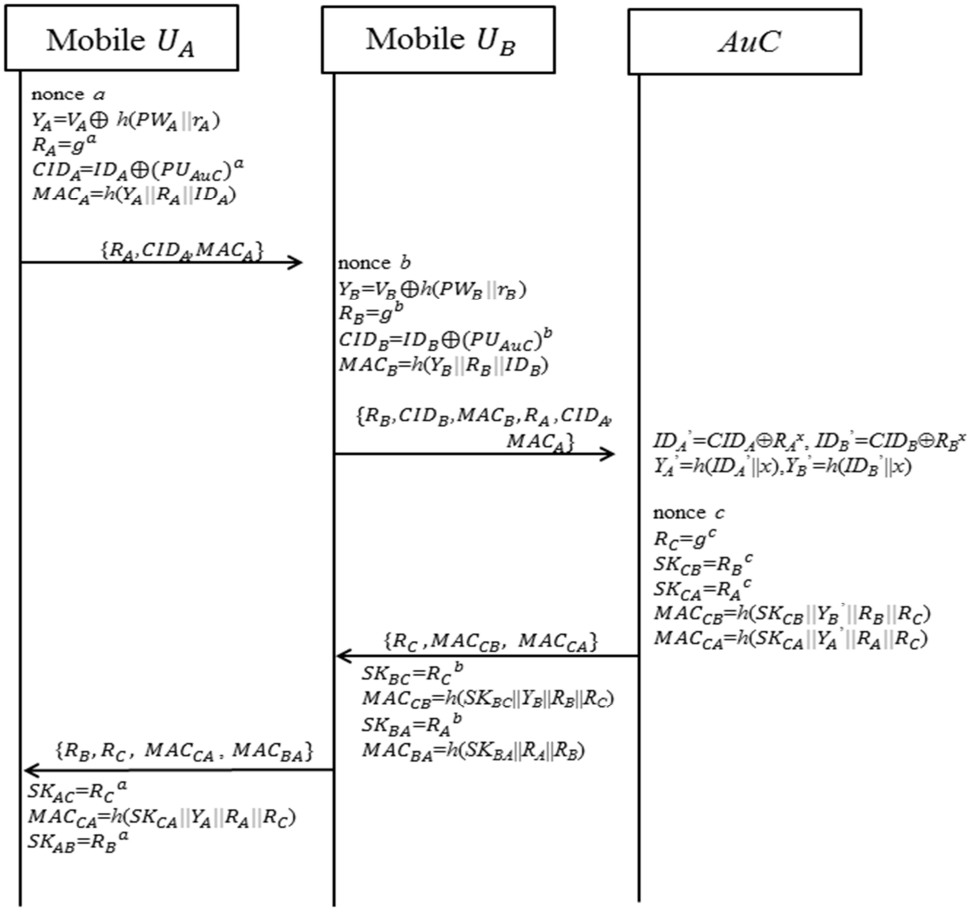

Fig. 3. Authenticated key agreement phase.

$$R_C = g^c \tag{16}$$

$$SK_{CA} = {R_A}^c \tag{17}$$

$$SK_{CB} = {R_B}^c \tag{18}$$

$$MAC_{CA} = h(SK_{CA}||{Y_A}'||R_A||R_C) \tag{19}$$

$$MAC_{CB} = h(SK_{CB}||{Y_B}'||R_B||R_C) \tag{20}$$

- [AP 4] $U_B \rightarrow U_A$

U_B verifies MAC_{CB} by computing SK_{BC} as in (21). For the verification, it compares MAC_{CB} with $h(SK_{BC}||Y_B||R_B||R_C)$. Only if the verification is successful, it computes SK_{BA} as in (22) and MAC_{BA} as in (23). After that, he (or she) sends $\{R_C, MAC_{CA}, MAC_{BA}, R_B\}$ to U_A.

$$SK_{BC} = {R_C}^b \tag{21}$$

$$SK_{BA} = {R_A}^b \tag{22}$$

$$MAC_{BA} = h(SK_{BA}||R_A||R_B) \tag{23}$$

- [AP 5] U_A

U_A verifies MAC_{CA} by computing SK_{AC} as in (24). For the verification, it compares MAC_{CA} with $h(SK_{AC}||Y_A||R_A||R_C)$. Only if the verification is successful, it also verifies MAC_{BA} by comparing with $h(SK_{AB}||R_A||R_B)$ after computing SK_{AB} as in (25). U_A believes that U_B is legal user and has the same session key with him (or her).

$$SK_{AC} = {R_C}^a \tag{24}$$

$$SK_{AB} = {R_B}^a \tag{25}$$

4. Security Analysis

This section examines that the AKA_{NFC} is secure under the NFC. Attacks are considered for user impersonation, password guessing and replay. Furthermore, we consider two considerable properties analysis focused on providing user anonymity and forward secrecy.

4.1. Resistant to User Impersonation Attack

The transmitted messages $\{R_A, CID_A, MAC_A\}$, $\{R_B, CID_B, MAC_B, R_A, CID_A, MAC_A\}$, $\{R_C, MAC_{CB}, MAC_{CA}\}$ and $\{R_B, R_C, MAC_{CA}, MAC_{BA}\}$ are all protected by secure one-way hash function and discrete logarithm problem. When certain modifications are performed by an attacker to these parameters of legitimated authentication messages from legal user A or B, the modifications could be detected by AuC. Although the attacker can change the values of R_A, CID_A, MAC_A, R_B, CID_B, MAC_B, R_C, MAC_{CA}, MAC_{CB} and MAC_{BA}, the attacker does not know any information about A, B, C and PW_i due to the one-wayness of the hash function and the discrete logarithm problem. Therefore, the attacker cannot fabricate the valid R_A, CID_A, MAC_A, R_B, CID_B, MAC_B, R_C, MAC_{CA}, MAC_{CB} and MAC_{BA}. Hence, the AKA_{NFC} is secure against user impersonation attack.

4.2. Resistant to Password Guessing Attack

One of the most important security requirements for password-based authentication protocols is to resist against password guessing attack. The user usually tends to select passwords with easy-to-remember,

which has low entropy. Hence, these passwords are potentially vulnerable to password guessing attack. Thereby, the AKA_{NFC} should not use any password related information in message transmissions. Even if the attacker could read the NFC, there is no way that the attacker knows APW_i related with the password PW_i due to one-wayness of the hash function $H()$. Therefore, the AKA_{NFC} is secure against password guessing attack.

4.3. Resistant to Replay Attack

The AKA_{NFC} is secure against replay attack because the login and key agreement messages $\{R_A, CID_A, MAC_A\}$, $\{R_B, CID_B, MAC_B, R_A, CID_A, MAC_A\}$, $\{R_C, MAC_{CB}, MAC_{CA}\}$ and $\{R_B, R_C, MAC_{CA}, MAC_{BA}\}$ are secured by using secure one-way hash function and discrete logarithm problem and by adopting session dependent fresh random numbers a, b and c. AuC could check the freshness of session dependent random number related values R_A or R_B in the authentication message. Furthermore, the attacker cannot compute session key related information due to the lack of knowledge related with a or b. Thereby, the AKA_{NFC} is secure against replay attack.

4.4. Provides User Anonymity

Attacker could get the messages $\{R_A, CID_A, MAC_A\}$, $\{R_B, CID_B, MAC_B, R_A, CID_A, MAC_A\}$, $\{R_C, MAC_{CB}, MAC_{CA}\}$ and $\{R_B, R_C, MAC_{CA}, MAC_{BA}\}$ by listening the network. However, there is no useful information from them to know about identification for the protocol participants. CID_A and CID_B are the only information related with the identification. However, they are secured by using session dependent random number and discrete logarithm problem. Thereby, the AKA_{NFC} provides anonymity.

4.5. Forward Secrecy

It is necessary to have an assumption that attacker could get the system's long term secret key x as usual for the forward secrecy. From the messages $\{R_A, CID_A, MAC_A\}$, $\{R_B, CID_B, MAC_B, R_A, CID_A, MAC_A\}$, $\{R_C, MAC_{CB}, MAC_{CA}\}$ and $\{R_B, R_C, MAC_{CA}, MAC_{BA}\}$, attacker needs to know about random numbers a and b from R_A and R_B, respectively, which are dependent with the session. However, it is impossible due to discrete logarithm problem. Thereby, the AKA_{NFC} provides forward secrecy.

5. Conclusion

This paper has been proposed a new authenticated key agreement based on NFC for mobile payment to solve the problems in the previous researches. We considered a scenario of three parties in the AKA_{NFC}, which are two end users whom share a common authentication server. Two end users could be a buyer or a seller at any period of time, respectively, which does not have any credential in between. Thereby, the authentication server could help them to be authenticated and key establishment between each other. Security analyses showed that the proposed scheme is secure against various attacks and could provide privacy to the participants.

Acknowledgment

This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2011-0008890) and also was supported by the National Research Foundation of Korea Grant funded by the Korean Government (MEST) (NRF-2010-0021575).

References

[1] Leishman, P. (2010). *Mobile Money for the Unbanked*. GSMA.

[2] Deloitte. (2012). Trends and prospects of mobile payment industry in China 2012-2015 creating

innovative models. *Boosting Mobile Financial Services*.
[3] Wikipedia: Mobile payment. From http://en.wikipedia.org/wiki/Mobile_payment
[4] PCI Security Standard Council. (2014). *Accepting Mobile Payments with a Smartphone or Tablet.*
[5] SANS Institute. Security of mobile banking and payments. 2012.
[6] Tiejun, P., *et al*. (2014). Research of mobile payment system based on external security device. *J. of Convergence Information Technology*, *9(2)*, 194-204.
[7] (2010). Nokia Money Pilot Begins in India. From http://conversations.nokia.com/2010/02/15/nokia-money-pilot-begins-in-india-video/
[8] Morawczynski, O., & Miscione, G. (2008). Examining trust in mobile banking transactions: The case of M-PESA in Kenya. *Pretoria: Human Choice and Computers* (pp. 287-298).
[9] SANS Institute. Strong user authentication for electronic and mobile commerce. Version 1.4.
[10] Han, S., Choi, O., Kim, K., Yeh, H., & Shon, T. (2012). A design of electronic payment authentication method based on NFC smartphone. *Proceedings of Information Security and Assurance* (pp. 38-40).
[11] Yadav, S., Patil, P., Shinde, M., & Rane, P. (2014). Android-based mobile payment system using 3 factor authentications. *Int. J. of Emerging Technology and Advanced Engineering*, *4(3)*, 797-801.
[12] Parte, S., *et al.* (2014). Study and implementation of multi-criterion authentication approach to secure mobile payment system. *Int. J. of Engineering Science & Advanced Technology*, *3(3)*, 117-122.
[13] Lee, Y., *et al.* (2013). A NFC based authentication method for defense of the man in the middle attack. *Proceedings of 3rd Int. Conference on Computer Science and Information Technology* (pp. 10-13).

Bomi Seo is a student at the Department of Cyber Security Kyungil University, Republic of Korea from 2013. She is interested in financial security and the recent security issues.

Sung Woon Lee is a professor at the Department of Information Security, Tongmyong University, Korea. He received the B.S. and M.S. degrees in computer science from Chonnam National University, Korea in 1994 and 1996, respectively, and the Ph.D. degree in computer engineering from Kyungpook National University, Korea, in 2005. He was with the Korea Information System as a researcher, Korea, from 1996 to 2000. His research interests include cryptography, network security, and security protocol.

Hyunsung Kim is a professor at the Department of Cyber Security, Kyungil University, Korea. He received his M.S. and Ph.D. degrees in computer engineering from Kyungpook National University, Republic of Korea, in 1998 and 2002, respectively. From 2000 to 2002, he worked as a senior researcher at Ditto Technology. He had been an associate professor from 2002 to 2011 with the Department of Computer Engineering, Kyungil University. He had been a visiting scholar from 2009 to 2010 with the School of Computing, Dublin City University, Ireland. Currently, he is a full professor at the Department of Cyber Security, Kyungil University. His current research interests are cryptography, VLSI, authentication technologies, network security and ubiquitous computing security.